

Recommendations for Improved DIB Cybersecurity



Dr. Eric Cole
SVP & CTO of the Americas

eric_cole@mcafee.com

April 7th, 2010



About Dr. Eric Cole




- Previous Federal Cybersecurity Official (IC)
- Previous cybersecurity chief scientist at major DIB corporation
- Member of commission on cyber security for the 44th President
- Performed security assessment, analysis and network designs for several large DOD and federal agencies
- As McAfee CTO Americas has visibility into best practices from all major sectors of economy (ex. Financial Services, CI/KR, Government, DIB)

- Our recommendations are based on proven best practices drawn from throughout society, not just .gov and .dib
- While much has been done, much more can be done
- No silver bullets
- Security is about mission enablement and incident cost avoidance
- As a subcontractor to many DIB primes, we too would be subject to proposed DFARS

- The threat environment is changing
More stealthy, constantly changing, encrypted, hybrid
- Requires a new approach to managing and controlling vulnerabilities
- Signature approaches no longer scale
- Look at outbound traffic performing clipping level analysis
- Internal threat as important as the external threat

A 21st Century Approach to Cybersecurity



- 
- A low-angle photograph of a modern glass skyscraper, showing its reflective surface and structural details against a blue sky with light clouds.
- Common security posture baseline and regular re-assessment of people, process and technology
 - Common training and certification regimes (SANS, ISC, DoD 8570)
 - Common process best practices – ITIL, ISO, CAG
 - Adoption of proven defense-in-depth security architectures – NIST, DoD
 - Enhanced situational awareness, continuous monitoring and real time actionable global threat intelligence (GTI) drawn from within .mil, .gov, .dib, and worldwide

Conclusion – Securing the Government



- Focus on data and protection of information
 - Data is more portable
 - Virtualization
 - Cloud computing
- Continue to secure the endpoint
 - Complement traditional measures with behavioral HIPS (host based intrusion prevention)
- Move security to virtualized environments
- Secure the cloud
- Prevention is ideal but detection is a must
 - Attacks are going to happen
 - Focus on timely detection in cases where prevention is not possible
- Mission resilience

THANK YOU FOR YOUR TIME